REMARKS

Claims 1-33 are pending, with claims 1, 13, 22, 24, 26, and 31 being independent. Reconsideration and allowance of the above-referenced application are respectfully requested.

Claims 1-33 are rejected under 35 U.S.C. 102(e) as being U.S. Patent Publication 2003/0126468 B1 (hereinafter Markham) with priority under 35 U. S. C § 119(a) based on PCT No. PCT/US01/17153 (WO 200191418 A2 November 29, 2001). This contention is respectfully traversed.

Markham is directed to "a system and method of enforcing a security policy by distributing aspects of the security policy across a number of devices while retaining the ability to react to attacks and to changes in the computing environment." (*See* Markham at ¶ 10.) Markham describes distribution of firewall functionality to independent components of host systems in a network, and providing centralized management of the distributed firewall integrated with autonomic response systems. (*See* Markham at ¶ 35.) If a particular host becomes compromised, the centralized management can update remaining hosts to not allow any more network traffic either to or from the compromised host. (*See* Markham at ¶s 31-32.) Moreover, the chances of denial of service attacks are minimized by proactive policies that require authentication of the source of network traffic. (*See* Markham at ¶s 33-34.)

In contrast, the present application describes integrating firewall functionality with intrusion detection on end nodes in a network using application-specific network policies. (*See* Specification at ¶s 21-22 and 25-26.) This enables increased specificity with respect to designating authorized network communications, and can result in significantly improved network intrusion detection, e.g., an application-specific network policy can be used to track application behavior and identify abnormal behavior specific to one application. (*See* Specification at ¶ 38.)

Independent claim 1 recites, "receiving requests for network communication services from an invoked application; selectively designating each of the received requests as authorized or unauthorized based on an application-specific network policy; and monitoring inbound network communications, based on the authorized requests, to detect an intrusion." (Emphasis added.) Markham fails to teach or suggest application-specific network policies, or use of such in selectively designating requests for network communication services from an invoked application as authorized or unauthorized. In Markham, the policies and communication authorization are specific to particular hosts, not to particular invoked applications. (*See* Markham at ¶s 46, 76, 108, and 130.) For at least these reasons, independent claim 1 should be in condition for allowance.

Independent claims 13, 22, 24, and 26 cover subject matter that also includes use of an application-specific network policy. Thus, for at least the above reasons, independent claims 13, 22, 24, and 26 should be in condition for allowance.

Moreover, independent claims 13 and 26 recite, "initiating monitoring of network communications for the invoked application using an application-specific intrusion signature in response to one or more unauthorized requests." (Emphasis added.) Markham does not describe application-specific intrusion signatures, nor using such in response to one or more unauthorized requests for network communication services from an invoked application. Claims 13 and 26 should be in condition for allowance for at least these additional reasons.

Independent claim 31 recites, "blocking inbound network communications that fail to correspond to a network policy; detecting a potential intrusion prelude from the blocked inbound network communications; selectively generating a fabricated response to the detected potential intrusion prelude; and receiving information about a potential intruder in response to the generated fabricated response." (Emphasis added.) Generation of a fabricated response is described in detail in the present specification. (*See e.g.*, Specification at ¶ 47.) Markham neither teaches nor suggests this feature, and the Official Action fails to address this feature of the claimed subject matter. For at least this reason, independent claim 31 should be in condition for allowance.

Dependent claims 2-12, 14-21, 23-24, 27-30, and 32-33 should be patentable based on the above arguments and the additional recitations they contain.

For example, claim 2 recites, "blocking the inbound network communications that fail to correspond to an authorized request; and monitoring the blocked inbound network communications to detect an intrusion." (Emphasis added.) Markham describes use of intrusion detection, including doing intrusion detection management at a master device (LSS 20) and doing intrusion detection at an end node (NIC 14). (*See* Markham at ¶s 36 and 45.) However, Markham does not describe designating a request for communication services from an invoked application as authorized or unauthorized, blocking inbound communications that fail to correspond to an authorized request, and monitoring the blocked inbound communications to detect an intrusion. This claimed subject matter can result in a significant reduction in the overall amount of network traffic that needs to be monitored to detect intrusions. (*See* Specification at ¶ 20.) Claims 2, 13, 26, and 32 should be allowable for at least these additional reasons.

Claims 3, 14, 27, and 33 recite, "examining the blocked inbound network communications to detect an intrusion prelude; identifying a source for a detected intrusion prelude; and initiating monitoring of inbound network communications from the identified source." (Emphasis added.) An "intrusion prelude" is defined in the present specification as "communication activities that typically precede an intrusion." (*See* Specification at ¶ 19.) Markham does not address intrusion preludes, nor does Markham describe responding to a detected intrusion prelude by identifying a source and initiating monitoring of inbound network communications from that identified source.

The cited portions of Markham describe blocking of all traffic for a compromised host and prevention of address spoofing. (See Markham at ¶s 32 and 34.) Markham neither teaches nor suggests detecting an intrusion prelude and then singling out a source of that intrusion prelude for greater scrutiny. Thus, claims 3, 14, 27, and 33 should be allowable for at least these additional reasons.

Claims 5, 17, and 25 should also be allowable in view of the arguments presented above in connection with claim 31 regarding fabricated responses.

Claims 7 and 8 should also be allowable in view of the arguments presented above in connection with claims 13 and 26.

Furthermore, claims 9, 12, 15, 19, 28, and 30 should be allowable because Markham does not describe identifying an invoked application by examining a set of instructions embodying the invoked application. The cited portions of Markham (¶s 100 and 140-143) say nothing about examining application instructions (e.g., applying a hash function to the invoked application's executable) to identify an invoked application. Thus, claims 9, 12, 15, 19, 28, and 30 should be allowable for at least these additional reasons.

Finally, for claims 10, 11, 20, and 21, the cited portions of Markham (¶s 104-106) describe storing a filter rule set in a portion of non-volatile memory (on NIC 14 and device 30) that is protected from host manipulation. Nothing is stated here regarding monitoring network communications for an invoked application in an intrusion detection system component invoked with the invoked application, let alone running the intrusion detection system component and the invoked application in a single execution context. Thus, claims 10, 11, 20, and 21 should be allowable for at least these additional reasons.

It is believed that all of the pending claims have been addressed. However, the absence of a reply to a specific issue or comment does not signify agreement with or concession of that issue or comment. Because the arguments made above may not be exhaustive, there may be reasons for patentability of any or all pending claims (or other claims) that have not been expressed. Finally, nothing in this paper should be construed as an intent to concede any issue with regard to any claim, except as specifically stated in this paper, and the amendment of any claim does not necessarily signify concession of unpatentability of the claim prior to its amendment.

It is respectfully suggested for all of these reasons, that the current rejections are overcome, that none of the cited art teaches or suggests the features which are claimed, and therefore that all of these claims should be in condition for allowance. A formal notice of allowance is thus respectfully requested.

Please apply any necessary charges or credits to Deposit Account No. 06-1050.

Respectfully submitted,

Date: October 26, 2005

William E. Hunter
Reg. No. 47,671

Fish & Richardson P.C.
12390 El Camino Real
San Diego, California 92130
Telephone: (858) 678-5070
Facsimile: (858) 678-5099

10552578.doc